Directiva

Protección de datos

13 septiembre, 2018

Contenido:

La Directiva General de Protección de Datos de Holcim es una parte integral del panorama de Directivas de Holcim. Esta directiva debe ser leída en estrecha colaboración con las políticas y directivas de Holcim enumeradas en el Anexo 2.

1.1 Aplicabilidad de la presente Directiva de Protección de Datos

1.1 Holcim Ltd y sus filiales consolidadas

Esta Directiva General de Protección de Datos se aplica a todos los oficiales, directores y empleados de todos los grados y niveles, y a otro personal, incluyendo personal temporal o contratado, becarios, segundas personas y consultores (en conjunto "Personal de Holcim") de Holcim Ltd y sus compañías consolidadas afiliadas al grupo ("Holcim" o el "Grupo")

El personal de Holcim debe familiarizarse con esta Directiva y cumplirla plenamente cuando realice cualquier actividad de protección de datos.

1.2 Empresas/ Joint Ventures

En las empresas asociadas o empresas mixtas en las que Holcim no ejerza el control accionarial o de gestión, el miembro responsable del Comité Ejecutivo del Grupo establecerá que la empresa asociada o la empresa mixta tiene conocimiento de esta Directiva y fomentará su adopción o, al menos, normas esencialmente equivalentes por parte de dicha empresa asociada o empresa mixta.

1.3 Terceras partes

Esta Directiva también debería ser vinculante para los proveedores de Holcim, los proveedores de servicios, otros socios comerciales y terceros en la medida en que presten servicios de procesamiento de datos para Holcim. Las disposiciones apropiadas deben ser incorporadas en cualquier servicio por parte de un contratista u otros acuerdos con tales terceros.

1.2 Contenido en el ámbito de aplicación

Esta Directiva establece el marco general de las normas y procedimientos de

protección de datos de Holcim. Debe leerse junto con las demás políticas, directrices y procedimientos pertinentes de Holcim relativos a la protección y seguridad de los datos, tal como se detalla en el Anexo 2 de la presente Directiva.

La Directiva define y explica las reglas y principios aplicados por Holcim al procesar los datos personales de nuestros empleados, clientes y cualquier otra persona que esté en contacto con nosotros. Describe cómo recogemos y procesamos los datos personales y qué procedimientos tenemos en marcha para proteger y salvaguardar dichos datos personales.

Si tiene alguna pregunta con respecto a esta Directiva, póngase en contacto con cualquier miembro del Equipo de Protección de Datos según se especifica a continuación.

2. Principios de la Directiva

2.1. Principios de procesamiento de datos justo

Los datos personales siempre serán

a) Procesados de forma legal, justa y transparente en relación con el sujeto de los datos (legalidad, justicia y transparencia);

b) recogidos para fines específicos, explícitos y legítimos y no tratados posteriormente de manera incompatible con dichos fines (limitación de la finalidad);

c) adecuados, pertinentes y limitados a lo que sea necesario en relación con los fines para los que se procesan (minimización de datos);

d) exactos y, cuando sea necesario, actualizados; los datos inexactos, en relación con los fines para los que se procesan, deben ser borrados o rectificados sin demora (exactitud);

e) almacenados sólo durante el tiempo necesario para los fines para los que se procesan o que de otra manera se permiten o requieren por la legislación aplicable (limitación del almacenamiento); y

f) Protegido contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental, utilizando medidas técnicas u organizativas adecuadas (integridad y confidencialidad)

2.2. Fundamentos legales

Los datos personales deben procesarse sobre la base de fundamentos jurídicos válidos. Los fundamentos jurídicos válidos se dan en la medida en que se aplique cualquiera de las siguientes condiciones:

a) Se ha obtenido el consentimiento del interesado.

b) El procesamiento es necesario para que Holcim cumpla con una obligación legal.

c) El procesamiento es necesario para que Holcim pueda llevar a cabo una tarea llevada a cabo en el interés público o en ejercicio de la autoridad oficial que se nos ha conferido.

d) El procesamiento es necesario para que Holcim realice o celebre un

contrato con el interesado.

e) El procesamiento es necesario para que Holcim proteja los intereses vitales del interesado o de otra persona.

f) El procesamiento es necesario para los fines de los intereses legítimos perseguidos por Holcim o un tercero, a menos que existan intereses, derechos o libertades primordiales del interesado.

2.3. Rendición de cuentas

Holcim ha establecido normas y procedimientos adecuados para demostrar la conformidad de sus actividades de tratamiento de datos con la legislación aplicable y la presente Directiva, en particular con los principios de tratamiento leal de los datos. Esto incluye, en particular, la documentación de las actividades de procesamiento en los Registros de Actividades de Procesamiento y la realización de evaluaciones de la privacidad de los datos cuando sea necesario (véase la Sección 10).

Cuando no se apliquen esas normas específicas, el personal de Holcim deberá crear y mantener la documentación apropiada que demuestre esa conformidad de sus actividades específicas de tratamiento de datos. Ésta debe incluir al menos cualquier información necesaria para demostrar

(a) Los fundamentos jurídicos y fines del tratamiento y

(b) el cumplimento de los principios de procesamiento justo establecidos anteriormente en esta sección .

El personal de Holcim debe notificar al responsable local de protección de datos cualquier actividad de procesamiento de datos personales y confirmar la idoneidad de su documentación.

3. Roles del usuarío y concepto de derecho de acceso

El acceso a cualquier dato personal procesado por Holcim debe limitarse estrictamente en función de la necesidad de conocerlo. El personal responsable de Holcim debe definir una función de usuario para cada función o grupo de funciones que tenga necesidad de acceder a los datos. El personal de Holcim que no pertenezca a una función de usuario no podrá acceder a los datos personales. El alcance del acceso debe ser diferenciado y limitado para cada función de usuario al alcance mínimo de los datos necesarios para los fines para los que se procesan los datos y las tareas y responsabilidades de la función de usuario pertinente. El concepto de derecho de acceso que detalla los derechos de acceso para cada función de usuario debe documentarse de manera transparente en forma escrita y debe estar fácilmente disponible para su examen e inspección. Los conceptos de derechos de acceso deben ser aprobados por el responsable local de protección de datos.

4. Datos sensibles y datos de los niños

4.1. Condiciones de procesamiento de datos

No obstante lo dispuesto en la sección 2.2 supra, los fundamentos jurídicos válidos

para el tratamiento de datos personales de niños menores de 16 años (u otro límite de edad definido en virtud de la legislación aplicable) o de datos sensibles (tal como se definen a continuación) sólo se dan si y en la medida en que se aplique cualquiera de las condiciones de tratamiento en virtud de la legislación aplicable, en particular si

a) El interesado ha dado su consentimiento explícito, a menos que la legislación aplicable nos prohíba confiar en dicho consentimiento.

b) Los datos personales pertinentes han sido manifiestamente hechos públicos por el interesado

c) El tratamiento es necesario para que Holcim pueda cumplir las obligaciones derivadas de la legislación laboral, de seguridad social o de protección social, o de un convenio colectivo.

d) El tratamiento es necesario para que Holcim pueda establecer, ejercer o defenderse de reclamaciones legales o cuando los tribunales actúen en su capacidad judicial.

El personal de Holcim debe ponerse en contacto con el Equipo de Protección de Datos y obtener la aprobación antes de comenzar cualquier procesamiento de datos de niños o Datos Sensibles. Cualquiera de estas actividades de procesamiento debe ser documentada en el Registro de Actividades de Procesamiento.

4.2. Definición

A los efectos de la presente Directiva, se entiende por "datos sensibles" los datos personales relativos al origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, la vida sexual o las orientaciones sexuales, los antecedentes penales, los datos sanitarios, los datos genéticos y los datos biométricos.

5. Toma de decisiones automatizada / Perfiles

5.1. Obligaciones legales

Holcim debe proteger los derechos de los individuos en relación con cualquier toma de decisiones automatizada, incluyendo la elaboración de perfiles. Esto se aplica a las siguientes situaciones:

a) Las decisiones de Holcim que producen efectos legales o que afectan de forma similar y significativa a los individuos se toman basándose únicamente en el procesamiento automatizado, es decir, sin ninguna intervención humana (toma de decisiones automatizada) o

b) Holcim utiliza datos personales para evaluar, analizar o predecir ciertos aspectos relativos al desempeño de un individuo en el trabajo, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento o la ubicación y el movimiento por medio de un procesamiento automatizado.

Las decisiones automatizadas sólo son admisibles si lo son:

a) Son necesarias para celebrar o ejecutar un contrato con el individuo,

b) autorizado por la ley aplicable; o

c) basado en el consentimiento explícito del individuo

5.2. Cómo cumplimos

Antes de que se procesen datos personales en cualquiera de las situaciones mencionadas, Holcim debe adoptar las salvaguardias adecuadas para proteger los derechos de las personas afectadas. El personal de Holcim debe notificar al Equipo de Protección de Datos cualquier actividad comercial que pueda implicar la toma de decisiones o la elaboración de perfiles automatizados.

El Equipo de Protección de Datos aprueba la actividad de procesamiento sólo si se implementan y documentan los siguientes procesos:

a) Se informa específicamente a los individuos sobre la toma de decisiones automatizada y la lógica que la sustenta.
b) Las personas tienen derecho a obtener la intervención humana, expresar su punto de vista y solicitar que se les explique la decisión adoptada.
c) Los individuos tienen derecho a impugnar la decisión

6. Información a los sujetos interesados

6.1. Nuestras obligaciones legales

Cuando los datos personales relativos a un interesado se recaben del interesado o de un tercero, Holcim deberá facilitar al interesado determinada información, según se define en la legislación aplicable, de forma concisa, transparente, inteligible y fácilmente accesible, utilizando un lenguaje claro y sencillo, en particular para la información dirigida específicamente a un niño.

Por interesado se entiende una persona física identificada o identificable cuyos datos personales son objeto de tratamiento.

6.2. Cómo cumplimos

Holcim ha establecido procedimientos para asegurar que todas las personas interesadas sean informadas oportuna, completa y transparentemente de conformidad con la legislación aplicable. La información se proporciona a los interesados a través del Aviso General de Privacidad de Datos de Holcim, disponible en el sitio web de privacidad de datos de Holcim (página web de privacidad de datos de Holcim) y a través de información adicional proporcionada en circunstancias específicas según sea necesario y apropiado.

Los detalles y procedimientos se establecen en las directrices pertinentes de Holcim que deben ser observadas por todo el personal de Holcim. Toda información a los interesados debe ser aprobada por el Equipo de Protección de Datos. El personal de Holcim debe notificar con prontitud al Equipo de Protección de Datos si tiene dudas sobre si las personas afectadas están debidamente informadas sobre cualquiera de sus actividades de procesamiento de datos.

7. Derechos del sujeto interesado

7.1. Obligaciones legales

En determinadas circunstancias y con sujeción a ciertas excepciones, las personas cuyos datos personales están siendo procesados por Holcim (por ejemplo, empleados, clientes u otros socios comerciales) pueden tener los siguientes derechos en relación con sus datos personales en virtud de la legislación aplicable

a) Rectificación de datos personales inexactos o incompletos.

b) Restricción (pausa o detención) del tratamiento de sus datos personales.

c) Borrado (supresión) de sus datos personales.

d) Objeción al tratamiento de sus datos personales.

e) Portabilidad de los datos: Solicitar que sus datos personales se entreguen en un formato estructurado, de uso común y legible por máquina, ya sea a sí mismos o directamente a un tercero si es técnicamente factible.

7.2. Cómo cumplimos

Holcim ha establecido procedimientos para asegurar que Holcim cumpla con los derechos de los interesados y responda de manera oportuna, completa y transparente a cualquier solicitud de los interesados.

Los detalles y procedimientos se establecen en las directrices pertinentes de Holcim, que deben ser observadas por todo el personal de Holcim. El Equipo de Protección de Datos se encarga de atender y responder a las solicitudes de los interesados. El personal de Holcim debe notificar sin dilación indebida al Equipo de Protección de Datos cualquier solicitud de un interesado y cooperar con el Equipo de Protección de Datos de acuerdo con las directrices pertinentes. Las solicitudes de protección de datos se documentan y registran debidamente por el Equipo de Protección de Datos.

7.3. El tratamiento de los interesados y otras cuestiones de protección de datos

El Equipo de Protección de Datos se encarga exclusivamente de las solicitudes, quejas, reclamaciones, preguntas, peticiones y cualquier otra comunicación o trato con los interesados u otros terceros (por ejemplo, los medios de comunicación) en relación con los asuntos de protección de datos.

Cualquiera de estos asuntos debe ser comunicado inmediatamente al Equipo de Protección de Datos.

8. Marketing Directo

8.1. Se debe obtener el consentimiento expreso de las personas interesadas antes de enviar cualquier comunicación comercial a una persona (incluidas las personas de contacto que trabajan para una organización de clientes), a menos que

a) hemos obtenido los datos de contacto de dicha persona durante un pedido anterior y la comercialización se refiere a productos y servicios similares a los pedidos anteriores y

b) el individuo no se ha opuesto expresamente a recibir comunicaciones comerciales y

c) se da al individuo la oportunidad clara y distintiva de objetar cualquier comunicación comercial, de forma gratuita y fácil.

8.2. Por lo tanto, el personal de Holcim debe cumplir con las siguientes reglas antes de enviar cualquier material publicitario o de marketing a personas específicas:

a) No debe enviar material de marketing por correo electrónico a menos que el destinatario haya dado su consentimiento expreso por adelantado o que Holcim haya obtenido su dirección de correo electrónico en el curso de la prestación de productos o servicios similares a ellos (o en el curso de la negociación para hacerlo).

b) El consentimiento del individuo (permiso de comercialización) debe ser obtenido para cualquier canal de comunicación relevante que pretenda utilizar (por ejemplo, correo electrónico, llamadas telefónicas y SMS) y debe estar clara y adecuadamente documentado para demostrar el cumplimiento y manejar las objeciones. Los formularios de consentimiento y los mecanismos para almacenar y documentar el consentimiento deben ser aprobados por el Equipo Jurídico y de Protección de Datos.

c) Debe asegurarse de que no se contacte a las personas que nos han notificado que no desean recibir material de marketing o que han retirado su consentimiento. Se deben mantener registros apropiados de referencia para asegurar que Holcim cumple con esta obligación.

d) Cualquier mensaje de marketing directo debe dar al individuo la oportunidad de oponerse a cualquier comunicación de marketing, de forma clara y distintiva, de forma gratuita y fácil. La redacción pertinente debe ser aprobada por el Equipo Jurídico y de Protección de Datos.

9. Transferencia de datos personales

Los datos personales pueden transferirse a destinatarios dentro del Grupo Holcim o a terceros sólo en la medida en que dicha transferencia esté permitida por la legislación aplicable, sea necesaria y apropiada.

Holcim ha establecido una Guía de Transferencia de Datos que describe detalladamente los requisitos legales para las transferencias de datos y los procedimientos que debe observar el personal de Holcim.

En particular, las siguientes normas se aplican a las transferencias de datos personales:

9.1. Transferencias a terceros

Holcim ha establecido procedimientos para garantizar que toda transferencia de datos personales a un tercero receptor, ya sea que actúe como procesador en nombre de Holcim o como controlador, cumpla con la ley aplicable. En particular, toda transferencia de datos de este tipo debe basarse en un acuerdo de procesamiento de datos adecuado que cumpla con los requisitos de la legislación aplicable. Estos requisitos se aplican en particular cuando contratamos a terceros vendedores y proveedores de servicios (como proveedores de servicios de IT, proveedores de nóminas, autónomos de IT o empresas de destrucción de datos) que procesan datos personales en nuestro nombre.

Holcim ha establecido directrices sobre la contratación de proveedores y la celebración de contratos de procesamiento de datos con los receptores de datos personales que explican cómo identificar las transferencias de datos y los requisitos legales para los acuerdos de procesamiento requeridos. También establecen los procedimientos aplicables de Holcim que deben ser observados por todo el personal de Holcim.

El Equipo de Protección de Datos y las funciones jurídicas de Holcim se encargan de prestar apoyo al personal de Holcim en la identificación de las situaciones de transferencia de datos, la evaluación de si se permite una transferencia de datos y la concertación de los acuerdos contractuales apropiados. Tales acuerdos deben obligar a los terceros proveedores que procesan datos personales en nuestro nombre a cumplir con esta Directiva en consecuencia.

El personal de Holcim debe notificar rápidamente al Equipo de Protección de Datos cualquier situación de transferencia de datos y cualquier acuerdo de transferencia de datos que se haya concluido. Los acuerdos de transferencia de datos deben estar debidamente documentados y registrados.

9.2. Transferencias transfronterizas

La transferencia de datos personales a un destinatario situado en un país fuera de la UE/EEE que no ofrezca garantías adecuadas de protección de los datos, sólo es admisible si se adoptan garantías adicionales aceptadas en virtud de la legislación aplicable. Esas salvaguardias incluyen, en particular, acordar con el receptor las cláusulas contractuales estándar adoptadas por la Comisión Europea o instrumentos jurídicos similares aprobados por una autoridad de supervisión.

El personal de Holcim debe cumplir con los procedimientos específicos para las transferencias de datos transfronterizas establecidos en las Directrices de transferencia de datos de Holcim.

9.3. Transferencias intra-grupo

Los principios anteriores se aplican a las transferencias de datos personales entre las filiales del Grupo Holcim ("Transferencias dentro del grupo") en consecuencia, ya que no existe un privilegio legal para dichas transferencias.

A fin de evitar una multitud de acuerdos bilaterales, Holcim ha establecido un Acuerdo de transferencia de datos dentro del grupo que abarca los principales flujos de datos dentro del grupo y sirve para cumplir los requisitos de responsabilidad y documentación en virtud de la legislación de protección de datos aplicable.

Antes de iniciar cualquier actividad comercial que pueda dar lugar a una Transferencia Intragrupo, el personal de Holcim debe notificar al Equipo de Protección de Datos. El Equipo de Protección de Datos confirmará si la transferencia de datos está permitida por la legislación aplicable, cubierta por el Acuerdo de Transferencia de Datos Intra-Grupo y hará cualquier enmienda al Acuerdo de Transferencia de Datos Intra-Grupo que pueda ser requerida.

10. Registro de las actividades de procesamiento

10.1. Mantenimiento de los registros de Holcim

Holcim mantiene registros de las actividades de procesamiento de datos personales en la medida en que lo exige la legislación aplicable y de conformidad con la legislación aplicable para cada entidad jurídica del Grupo Holcim.

El Equipo de Protección de Datos se encarga de mantener y actualizar los registros

10.2. Notificación de las actividades de elaboración

Holcim Los miembros del personal y las funciones de organización (por ejemplo, RR.HH., Ventas, IT, Seguridad de IT, Contabilidad) que utilicen, patrocinen, supervisen, gestionen o participen de alguna otra manera en una actividad de procesamiento deben notificar al Equipo de Protección de Datos la actividad de procesamiento lo antes posible (por ejemplo, ya en la fase de planificación de un proyecto). En caso de duda, el personal de Holcim debe ponerse en contacto con el Equipo de Protección de Datos para obtener orientación sobre si una actividad de procesamiento debe incluirse en los registros.

Una actividad de procesamiento es cualquier actividad comercial, tecnologíca, producto, servicio, sistema o aplicación informática y cualquier otra actividad que implique el procesamiento de datos personales.

Ejemplos: Nuevos productos que procesan datos personales (por ejemplo, un medidor inteligente), un sistema de vigilancia por cámara, un sistema de control de acceso, una nueva base de datos de clientes, un nuevo sistema de evaluación del rendimiento de los empleados, la localización por GPS de los vehículos de la empresa, un sistema de pago sin dinero en efectivo para la cafetería, la subcontratación de actividades o funciones a un tercero

11. Prevención de "Shadow IT"

El personal de Holcim no está autorizado a participar en ningún procesamiento de datos personales que no haya sido revisado para cumplir con la ley de protección de datos y aprobado por el Equipo de Protección de Datos (también conocido como "Shadow IT").

Shadow IT puede exponer a Holcim a importantes riesgos legales, de reputación y financieros por las siguientes razones:

a) Shadow IT no está incluido en el registro de actividades de procesamiento y, por lo tanto, no puede incluirse en las respuestas a las solicitudes de los interesados.

b) No se supervisa ni se garantiza el cumplimiento de los requisitos de la ley de protección de datos.

c) Las infracciones de datos en Shadow IT no se supervisan y, por lo tanto, no se pueden comunicar oportunamente a las autoridades o a los interesados.

d) Las normas de seguridad de los datos pueden no estar a la altura de las normas de Holcim.

12. Evaluaciones del impacto de la protección de datos

12.1. Nuestras obligaciones legales

Si así lo exige la legislación aplicable, las entidades de Holcim llevarán a cabo y documentarán una evaluación del impacto de la protección de datos ("DPIA") para ciertos tipos de actividades de procesamiento de datos de "alto riesgo".

La DPIA es una "evaluación del impacto de una actividad de procesamiento de datos prevista en la protección de los datos personales". Sólo se requiere si una actividad "puede dar lugar a un alto riesgo para los derechos y libertades de las personas físicas

12.2. Cómo cumplimos

Holcim ha desarrollado un proceso de DPIA sobre la base de la orientación de las autoridades de supervisión, que es administrado por el Equipo de Protección de Datos y apoyado por los propietarios y el personal que participan en las actividades de procesamiento pertinentes. Los detalles y el proceso se definen en las Directrices de la DPIA de Holcim, que deben ser cumplidas por el personal de Holcim.

Los miembros del personal de Holcim que poseen o participan en una actividad de procesamiento que pueda requerir una DPIA deben notificarlo al Equipo de Protección de Datos lo antes posible (por ejemplo, ya en la fase de planificación de un proyecto). La DPIA debe llevarse a cabo antes de iniciar la actividad de procesamiento. Debe iniciarse lo antes posible en el diseño de la operación de procesamiento, incluso si algunas de las operaciones de procesamiento son todavía desconocidas.

Ninguna actividad de procesamiento que pueda requerir una DPIA puede comenzar antes de la aprobación del Equipo de Protección de Datos y la finalización de la DPIA (cuando sea necesario).

El Equipo de Protección de Datos se encarga de documentar adecuadamente la DPIA y su resultado, incluida toda la información reunida, los riesgos identificados, el asesoramiento del Delegado de Protección de Datos (DPO), las decisiones y sus motivos, así como las medidas correctivas adoptadas.

El personal de Holcim sigue siendo el principal responsable de vigilar la actividad y notificar al Equipo de Protección de Datos cualquier cambio que pueda requerir una DPIA. El Equipo de Protección de Datos se encarga de determinar los ciclos de auditoría y actualización adecuados para confirmar el cumplimiento continuo de la actividad de procesamiento.

13. Directiva de retención y eliminación de datos

Los datos personales no pueden conservarse y almacenarse más tiempo del necesario. Esto significa que Holcim necesita borrar los datos personales cuando:

a) ya no se necesitan para los fines legítimos para los que fueron procesados,

b) ya no estamos obligados, en virtud de la legislación aplicable o por orden de una autoridad, a retenerlos y

c) no se aplica ninguna exención que requiera o permita que sigamos conservando los datos.

Normalmente se aplicará una exención si necesitamos los datos para el establecimiento, el ejercicio o la defensa de reclamaciones legales.

La Directiva de Retención y Eliminación de Datos de Holcim implementa estos requisitos legales que deben ser cumplidos por todo el personal de Holcim. La Directiva de retención y eliminación de datos de Holcim se complementa con políticas locales que definen los períodos de retención específicos aplicables a la jurisdicción o entidad pertinente y otras normas y procedimientos locales.

14. Privacidad por diseño y defecto

Privacy by Design & Default se aplica como principio para la legalidad del tratamiento de datos personales en virtud de la legislación aplicable.

La aplicación de la privacidad por diseño y por defecto en Holcim significa lo siguiente:

a) Privacidad por diseño: Desde el comienzo de cualquier nuevo servicio o proceso comercial que haga uso de datos personales debemos tomar medidas (como la seudonimización) para minimizar el procesamiento de datos personales y cumplir con los principios de las leyes de protección de datos (como la minimización de datos).

b) Privacidad por defecto: Debemos tomar medidas para garantizar que, por defecto, en cada actividad comercial sólo procesamos los datos personales que son necesarios, en la medida en que sea necesario, y sólo almacenamos los datos durante el tiempo necesario para el propósito.

Holcim ha establecido unas directrices de Privacy by Design & Default que dan al personal de Holcim una guía práctica sobre cómo aplicar Privacy by Design & Default en la práctica y explica los procedimientos relevantes de Holcim que deben ser observados por todo el personal de Holcim.

15. Seguridad de datos

15.1 Normas de seguridad de datos en Holcim

Holcim debe aplicar las medidas técnicas y organizativas más avanzadas para proteger la integridad y seguridad de los datos personales y evitar la destrucción, la pérdida, la alteración, la divulgación no autorizada o el acceso accidental o ilegal a los datos personales transmitidos, almacenados o procesados de otro modo.

Las normas de seguridad de datos aplicadas incluirán, entre otras cosas, lo siguiente

a) La seudonimización y el cifrado de los datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios de procesamiento;

c) la capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de incidente físico o técnico;

d) un proceso para probar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento.

Las normas de seguridad de los datos de Holcim se supervisarán constantemente y se auditarán periódicamente para comprobar que siguen siendo adecuadas y se ajustan a la legislación aplicable.

El Equipo de Protección de Datos es responsable de proporcionar la formación adecuada al personal de Holcim en relación con el cumplimiento de las políticas de seguridad de datos.

Los supervisores, el departamento de recursos humanos y otras funciones a cargo son responsables de hacer cumplir las políticas de seguridad de los datos y de garantizar que cualquier infracción dé lugar a la adopción de medidas disciplinarias apropiadas y a la prestación de capacitación o apoyo adicionales, cuando proceda.

16. Procedimiento de respuesta a la violación de datos

Holcim ha establecido un Procedimiento de Respuesta a la Violación de Datos que define los procesos y medidas a:

a) responder a una Violación de Datos, incluyendo los pasos y medidas inmediatas que deben tomarse cuando se identifica una Violación de Datos para mitigar cualquier daño y riesgo para Holcim o los individuos afectados, así como las funciones y responsabilidades para gestionar una respuesta a una Violación de Datos; y

b) cumplir con las obligaciones pertinentes de la Compañía en virtud de la legislación aplicable sobre privacidad y protección de datos, incluida la obligación de notificar oportunamente las infracciones de datos a las autoridades de supervisión o a las personas afectadas.

Una "Violación de datos" es cualquier violación real o presunta de la seguridad que lleve a la destrucción accidental o ilegal, la pérdida o la pérdida de acceso a, la alteración, la divulgación no autorizada o el acceso a, u otro uso indebido que implique a Holcim Data, en particular los datos personales.

Todo el personal de Holcim y cualquier contratista que procese datos personales en nombre de Holcim debe familiarizarse y cumplir con el Procedimiento de Respuesta a la Violación de Datos.

17. Incumplimiento de esta directiva

Todo el personal de Holcim debe familiarizarse y cumplir con esta Directiva. El incumplimiento de esta Directiva puede dar lugar a procedimientos disciplinarios y puede resultar en sanciones disciplinarias.

17.1 Documentación de apoyo

El Comité Ejecutivo del Grupo ordena al Comité de Protección de Datos de Holcim que adopte toda la documentación de apoyo necesaria para la aplicación de esta Directiva, como los procedimientos y directrices.

2. Requerimiento relacionados con MCS

Según los MCSs Control no. 11 (Protección de datos personales) versiones aplicables.

3. Reporte

1. A nivel corportativo

a) Comité Ejecutivo Grupo Holcim

El Comité Ejecutivo del Grupo aprueba la creación, modificación o suspensión de esta Directiva General de Protección de Datos.

b) Comité de Protección de Datos del grupo designado para cubrir el area de esta Directiva

El Asesor General del Grupo y el Oficial de Cumplimiento, el Director de Recursos Humanos del Grupo, el Director Financiero del Grupo y el Director de Información del Grupo son responsables del área cubierta por la Directiva General de Protección de Datos, de aprobar cualquier documentación de apoyo necesaria para la aplicación de esta Directiva, como los Procedimientos y Directrices, y de presentar los cambios de esta Directiva General de Protección de Datos a la aprobación del Comité Ejecutivo del Grupo.

c) Delegado de Protección de Datos del Grupo ("DPO") y la oficina de Gestión de Datos del Grupo

El Oficial de Protección de Datos del Grupo dirige la actividad de la Oficina de Gestión de Datos del Grupo y promueve el cumplimiento de la protección de datos y las mejores prácticas en el establecimiento y mantenimiento de normas y procedimientos en todo el Grupo. El responsable de protección de datos evalúa el marco de protección de datos existente para identificar posibles lagunas en los procesos de protección de datos en todas las filiales del Grupo.

El RPD asesora, supervisa e informa sobre la aplicación de esta Directiva, mantiene, propone enmiendas y revisa, cuando es necesario, la Directiva General de Protección de Datos del Grupo y su documentación de apoyo (Directivas, Procedimientos, Directrices).

El RPD actúa como responsable independiente de la protección de datos de acuerdo con las leyes de protección de datos pertinentes, incluidas, entre otras, la Ley Federal de Protección de Datos de Suiza (DSG) y el Reglamento General de Protección de Datos de la Unión Europea. Los responsables de la protección de datos designados localmente (cuando así lo exige la legislación aplicable), son funcionalmente responsables ante el RPD en el ámbito de la protección de datos

1. A nivel país CEO local

El Director General de cada país es responsable del cumplimiento de esta Directiva por parte de la Empresa del Grupo y delegará las responsabilidades de tareas específicas al responsable local de protección de datos y a las diferentes funciones y unidades organizativas.

CEO checklist – Cuando aplique

El CEO de cada país tiene que:

- Asegurar la aplicación del número de control de los MCS. 11
- Indicar a los responsables de las funciones correspondientes que apliquen las medidas técnicas y organizativas para proteger los datos personales procesados por la empresa y que documenten dichas medidas
- Indicar a los jefes de función correspondientes que se aseguren de que los empleados pertinentes bajo su supervisión reciban capacitación en materia de protección de datos en relación con sus responsabilidades laborales
- Asegurarse de que las infracciones de los datos se comuniquen y se adopten las medidas necesarias de manera oportuna, de conformidad con los requisitos de la legislación local.

Control del documento	
Aprobado por	Responsible Group Executive Committee Member: Jan Jenisch, Group Chief Executive Officer, Keith Carr, Group General Counsel Persona responsable: Christopher Wright, Head of Group Compliance; Catalin Olarescu, Head of Data Management Office
Directivas relacionadas	Directiva de usuario de sistemas de información

Control de la versión			
Versión número	fecha	Autor	Información actualizada
01	13 de septiembre de 2018	Catalin Olarescu, Head of Data Management Office	

02	28 de febrero de 2020	Catalin Olarescu, Head of Data Management Office	Reclasificado como Directiva. Introducción de la sección "Requisitos y MCSs relacionados".

Definiciones y abreviaturas

(Orden alfabetico)

BoD	Board of Directors. Comité ejecutivo
CEO	Chief Executive Officer. Director
CFO	Chief Financial Officer. Director financiero
CFT	Corporate Financing and Treasury
CH	Corporate Holding Companies, Corporate Holdings
CLCO	Chief Legal and Compliance Officer. Director del departamento legal y encargado de Cumplimiento/Compliance
DPO	Data Protection Officer. Delegado de protección de datos
DMO	Data Management Office
DPR	Data Protection Responsible. Responsible de protección de datos
Grupo	Grupo Holcim, refiriéndose al grupo consolidado que incluye todas las compañías de holding y operativas.
Empresa afiliada/filial del grupo	Se refiere a una compañía en la que Holcim tiene el control, independientemente de si es un Holding Corporativo o una Compañía Operativa. Cuando se denomina subsidiaria, comprende todos sus órganos de gobierno, incluyendo su junta, los comités de la junta y la dirección ejecutiva.
HR	Human Resources. Recursos Humanos
IDTA	Intra Group Data Transfer Agreement. Transferencia de datos intragrupo
MCS	Minimum Control Standards